We claim

1. A method of signing and authenticating a message m in a public key data communication system, comprising the steps of :

in a secure computer system;

(a) generating a first short term private key k;

(b) computing a first short term public key derived from said first short term private key k;

(c) computing a first signature component r by using said first short term public key k;

(d) generating a second short term private key t;

(e) computing a second signature component s by using said second short term private key t on said message m, said long term private key and said first signature component r;

(f) computing a third signature component c using said first and second short term private keys t and k respectively, and sending said signature components (r, s, c) as a masked digital signature of said message m to a receiver computer system; in said receiver system;

(g) using said second and third signature components (s,c) computing a normal signature component $\bar{s}$ and sending said signature components ($\bar{s}$, r) as a normal digital signature to a receiver verifer computer system; and in said verifier system

(h) verifying said normal signature.

2. A method as defined in claim 1, said first short term private key k is an integer and said first short term public key is derived by computing the value $kP = (x_1,y_1)$ wherein P is a point of prime order n in E(Fq), wherein E is an elliptic curve defined over F_q.

3. A method as defined in claim 2, said first signature component r having a form defined by $r = \bar{x} (\mathrm{mod}\, n)$ wherein $\bar{x}$ is derived by converting said coordinate x_1 to an integer $\bar{x}$.

4. A method as defined in claim 3, said second short term private key being an integer selected such that $2 \leq t \leq (n-2)$, and said second signature component being defined by $s = t(e + dr) \pmod{n}$, wherein e is a hash of said message m.

5. A method as defined in claim 4, said third signature component being defined by $c = tk \pmod{n}$.

6. A method as defined in claim 5, said normal signature component $\bar{s}$ being defined by $\bar{s} = c^{-1}s \bmod n$.

7. A method of generating a digital signature S of a message in a data communication system, wherein the signor of the message has a private key d and a public key y derived from an element g and said private key d, said method comprising the steps of:

(a) generating a short term private key k;

(b) computing a first short term public key derived from said short term private key k;

(c) computing a first signature component r by using said first short term public key k;

(d) generating a second short term private key t;

(e) computing a second signature component s by using said second short term private key t on said message m, said long term private key and first signature component r;

(f) computing a third signature component c using said first and second short term private keys t and k respectively;

(g) sending said signature components (r, s, c) as a masked digital signature of said message m to a receiver computer system.

8. A method as defined in claim 7 including the step of in said receiver computer system, using said second and third signature components (s, r) computing a normal

signature component $\bar{s}$, and sending said signature components ($\bar{s}$, r) as a normal digital signature to a verifier computer system, and verifying said normal signature (s, r) by said verifier system.

9. A method as defined in claim 8 including the step of in said receiver system, using said second and third signature components (s, c) computing a normal signature component $\bar{s}$, to derive a normal digital signature components ($\bar{s}$, r) and;
verifying said normal signature components.

10. A processing means for assigning a message m without performing inversion operations and including a long term private key contained within a secure boundary and a long term public key derived from said private key and a generator of predetermined order in a field, said processing means comprising:
within said secure boundary;
means for generating a first short term private key;
means for generating a second short term private key;
means for generating a first signature component using at least said second short term session key; and
generating a masked signature component using said first and second short term session keys to produce masked signature components of said message m.

11. A processing means as defined in claim 10, including means for converting said signature components to a normal signature component; and
means for transmitting said normal signature components to a recipient.